Notice of Allowability	Application No.	Applicant(s)	
	10/804,097	ENOKIDA, TOMOAKI	
	Examiner	Art Unit	
	Courtney D. Fields	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *19 March 2004*.

2. ☒ The allowed claim(s) is/are *1-77*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 3/19/2004
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. Claims 1-77 are pending.

Information Disclosure Statement

2. The Information Disclosure Statement respectfully submitted on 29 July 2004 has been considered by the Examiner.

Allowable Subject Matter

3. **Claims 1-77** are allowed.

4. The following is an examiner's statement of reasons for allowance: The present invention is directed towards a digital certificate management apparatus and method for updating a proof key used for proving validity of a digital certificate used for authentication for establishing communication between a client and a server. Each independent claims identifies the uniquely distinct features "**updating the proof key, proving validity of the digital certificate for mutual authentication, creating a new digital certificate, creating a new proof key, and transmitting the proof key and certificate through a special communication path**".

The closest prior art, Lord et al. (US Patent No. 7,131,003) discloses a secure instant messaging system integrates secure text instant messaging and secure file transfers into existing instant messaging systems. At least one certificate authority (CA) is provided that issues a security certificate to a user that binds the user's instant messaging screen name to a public key which is used by other users to encrypt

messages and files sent to the user and by the user to decrypt the received messages and files. A subscriber database is used by the CA to keep track of valid users and their associated information, such as: user screen names, user subscription expiration dates, and enrollment agent information. A user sends his certificate to the invention's instant messaging server which publishes the user's certificate to other users by creating a hash value of the user's certificate and sending it to the other users which allows the recipients to decide if they need to update their caches with a new copy of the user's certificate. Instant messages and files are encrypted by a sending user using an encryption algorithm and the recipient's certificate. The sending user can sign instant messages using his private signing key. The security status of each received instant message is displayed to the user. However, either singularly or in combination, Lord et al. fail to anticipate or render the above underlined limitations obvious.

The closest prior art, Guo et al. (Pub No. 2003/0217288) discloses a security protocol for use in a multi-site authentication system. After authenticating a user, an authentication server generates a ticket including information associated with the user. The authentication server encrypts content of the ticket using a symmetric key shared with an affiliate server. The affiliate server has a public key that the authentication server uses to encrypt the shared key. The authentication server has private key for creating a signature on the ticket. The affiliate server decrypts the shared key with its private key and then decrypts the content of the ticket using the decrypted shared key. The affiliate server validates the signature with the authentication server's public key.

However, either singularly or in combination, Guo et al. fail to anticipate or render the above underlined limitations obvious.

The closest prior art, Kakii (Pub No. 2005/0204164) discloses a method of transferring digital certificates for transferring, by means of a digital-certificate transferring apparatus, a digital certificate to a communications apparatus to be its communications counterpart is disclosed. The method includes the step of causing the digital-certificate transferring apparatus to execute; a first transferring procedure of using a common certificate being a digital certificate without apparatus-identifying information so as to authenticate the communications counterpart, and transferring a normal certificate being a digital certificate with information identifying the communications counterpart to the communications counterpart when the authenticating succeeds; and a second transferring procedure of receiving a first normal certificate from the communications counterpart, and when, based on the received first normal certificate, transferring a second normal certificate, with the information identifying the communications counterpart, and being different from the first normal certificate, is determined to be necessary, transferring the second normal certificate to the communications counterpart. However, either singularly or in combination, Kakii fail to anticipate or render the above underlined limitations obvious.

5. Therefore, **claims 1,4,6,16-19,22-23,33-36,39,41,51,54-55,65-71,** and the respective **dependent claims 2-3,5,7-15,20-21,24-32,37-38,40,42-50,52-53,56-64, and 72-77** are in condition for allowance.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cdf
September 20, 2007

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137